MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDERSECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF THE DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER
COMMANDERS OF THE UNIFIED COMBATANT COMMANDS

E2.1. SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 11-8450-_____-Department of Defense and Intelligence Community Enterprise Computing

The attached Department of Defense and Intelligence Community Enterprise Computing guidance and policy is effectively immediately. It establishes policies and assigns responsibilities to further achieve effective, efficient, and economical acquisition, management, and use of computing equipment and services.

This policy guidance establishes a holistic Enterprise Computing policy for the Department.

My point of contact for this effort is Lt Col Ronald Holloway, who can be reached at (703) 607-0506, or by email: Ronald.Holloway@osd.pentagon.mil.

Signature Block

Global Information Grid (GIG)
Enterprise Computing
Guidance and Policy Memorandum

1 PURPOSE: This Guidance and Policy Memorandum (G&PM) establishes Department of Defense (DoD) policy related to Enterprise Computing (personal, local, regional, and global computing) to enable the secure exchange and use of information necessary to the execution of the DoD mission. This policy is an extension of the Global Information Grid G&PM. This document establishes policies, guidance, and assigns responsibilities to:

1.1 Develop and maintain architectures that provide for the choice of the computing platform (from microcomputer to mid-tier to mainframe to supercomputer) and the placement of application and data while managing the diversity of the Enterprise computing environments.

1.2 Ensure information assurance and interoperability across these Enterprise Computing environments.

1.3 Provide for the coordination and synchronization of the planning, development, implementation, and operations of Enterprise Computing using the standard DoD requirements, resource allocation and acquisition processes.

1.4 Manage Enterprise Computing resources and service providers.

2 APPLICABILITY:

2.1 This guidance and policy applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2 This policy must comply with public law and established DoD and Director Central Intelligence (DCI) Directives relative to architecture, requirements, resource allocation, acquisition and security policies and practices. [Consider adding this to the Overarching and other G&PMs.]

3 SCOPE:

3.1 This Directive applies to all personal, local, regional and global computing environments, collectively referred to as Enterprise Computing, and service/agency and joint functional applications that are administered, managed, acquired, operated or used by the DoD Components. IT embedded in National Security Systems (NSS) shall comply with this policy. Interfaces with systems external to the DoD shall be in accordance with this policy to the maximum extent possible.

3.2 This Directive uses the Computing and Communications Architecture Framework Sub-view (CCAFS) that clarifies the scope and relationship of Enterprise Computing within a broader architectural context. See Enclosure (1) of this policy for an introduction to the CCAFS and its related terminology.

4 DEFINITIONS: See Enclosure (2)

5 POLICY: It is the policy of the DoD that:

5.1 Enterprise Computing Architecture Management

5.1.1 The foundation for Enterprise Computing shall be the GIG computing and communications architecture.

5.1.2 Enterprise Computing (personal, local, regional and global computing) environments shall be planned, designed, and implemented to support all DoD Components' applications and tools.

5.1.3 The appropriate computing platforms (from microcomputers to supercomputers) shall be available within each Enterprise Computing environments to meet information processing and storage requirements.

5.1.4 Each application shall use the appropriate standard application program interfaces.

5.1.5 Applications shall be designed to share end user devices.

5.1.6 Any application or associated data that is common to more than one operational site not utilizing a DoD designated regional or global computing centers shall require a waiver.

5.1.7 Regional computing environments shall be consolidated on a limited number of regional computing centers within a geographical area for operational effectiveness and cost efficiencies.

5.1.8 Global computing environments shall be consolidated on a limited number of global computing centers for operational effectiveness and cost efficiencies.

5.1.9 Personal and local computing environments shall be planned, designed, and implemented to maximize the use of standard configurations of end-user devices, local servers, local networks, user productivity tools, and associated software.

5.1.10 Regional and global computing environments shall be planned, designed, and implemented to maximize the use of standard configurations of regional servers, global servers, user productivity tools, development environments, and associated software.

5.1.11 All personal, local, regional, and global computing standard configurations shall be planned, designed, and implemented to use the enterprise network environments. These standard configurations shall support end-to-end interoperability of information assurance services, computer and network management services, and information distribution services for all DoD

Components' applications.

5.2 Enterprise Computing Resource and Acquisition Management

5.2.1 Component Business Case Analyses (BCA) and performance assessments shall be conducted to determine the optimal choice of computing platform, and placement of applications and associated data on personal, local, regional, and global servers.

5.2.2 Plans and programs for Enterprise Computing environments shall be coordinated and synchronized to ensure appropriate capacities and migration to approved architectures.

5.2.3 Component five-year IT investment strategies shall be reviewed annually to assure program synchronization for planned Enterprise Computing capabilities, for inclusion in the Program Objective Memorandum (POM) submission.

5.2.4 Component current year budget shall be reviewed annually to assure synchronization and architectural compliance for Enterprise Computing programs prior to execution.

5.2.5 Upgrades or expansions of legacy Enterprise Computing environments that do not conform to standard configurations shall be minimized and require a waiver.

5.2.6 DoD designated regional and global service providers shall have the right to compete for all regional and global computing workload.

5.2.7 Enterprise Computing service providers shall be chosen on a best value basis, unless mission requirements dictate otherwise.

5.2.8 All software shall be properly licensed before use.

5.2.9 Inventories of all hardware and software installed on Enterprise Computing environments shall be created and maintained.

5.3 Enterprise Computing Operations Management

5.3.1 Service Level Agreements (SLAs) shall be established with all computing service providers.

5.3.2 Enterprise Computing service providers shall be held accountable for their performance in accordance with their SLAs.

5.3.3 There shall be one Enterprise Computing coordinator for personal and local computing and communications environments within a military or civilian installation.

5.3.4 Enterprise Computing environments shall be designed, developed, tested and operated to ensure continuity of operations consistent with operational requirements.

5.3.5 Operational status of Enterprise Computing environments shall be made visible to the appropriate GIG operators and users.

5.3.6 All Enterprise Computing assets shall be disposed of according to existing

Federal and DoD policy.

6 RESPONSIBILITIES

6.1 DoD Chief Information Officer/Assistant Secretary of Defense (C3I):

6.1.1 Promulgate and issue guidance and instructions to this policy.

6.1.2 Develop and maintain the Enterprise Computing Architecture, including:

6.1.2.1 The CCAFS and associated reference models using an automated tool and repository.

6.1.2.2 The standard configurations for Enterprise Computing environments to accommodate:

6.1.2.2.1 End-to-End compatibility across information assurance, computer and network management and information distribution services.

6.1.2.2.2 Use of COTS and non-COTS products based on technical standards.

6.1.2.2.3 Insertion of technology to meet functional requirements (state-of-the-practice).

6.1.2.2.4 Implementation of new and emerging technologies (state-of-the-art).

6.1.2.3 The standard application program interfaces for each type of computing platform.

6.1.2.4 A testing and certification process to ensure standard configurations of hardware and software are interoperable with computing and network environments.

6.1.2.5 The waiver process for deviations from the Enterprise Computing architectures.

6.1.2.6 Automated tools and repositories for the creation, storage and dissemination of the enterprise architectures, associated reference models and equipment and software inventories.

6.1.3 Ensure that all regional and global computing environments and joint and special interest applications are in compliance with Enterprise Computing architectures.

6.1.4 Ensure that all acquisition agents conduct a Business Case Analysis and performance assessment to determine the optimal choice of computing platform and placement of joint or special interest applications and associated data on Enterprise Computing environments.

6.1.5 Review annually the five-year Enterprise Computing investment strategies prepared by Services and Agencies during the POM submission for alignment of priorities and synchronization of programs.

6.1.6 Provide for the elimination of duplicate regional and global computing environments across the DoD Components.

6.1.7 Establish certification authorities for regional and global computing architecture compliance.

6.1.8 Ensure all program/acquisition managers that develop or acquire joint or special interest applications or data of a regional or global nature use designated regional and global computing centers or obtain a waiver.

6.1.9 Establish consistent roles and responsibilities for Enterprise Computing service providers including specific performance measurements.

6.1.10 Establish a process for selecting, evaluating and accrediting designated regional and global computing service providers.

6.1.11 Arbitrate issues regarding non-performance of SLAs for the designated regional and global computing service providers.

6.1.12 Ensure that automated inventories of all current and planned Enterprise Computing assets are created and maintained.

6.2 Service/Agency Chief Information Officer

6.2.1 Promulgate and issue guidance and instructions to this policy.

6.2.2 Ensure that personal and local computing environments and all Service/Agency applications are in compliance with approved Enterprise Computing architectures.

6.2.3 Ensure that all acquisition agents conduct a Business Case Analysis and performance assessment to determine the optimal choice of computing platforms and placement of applications and associated data on personal, local, regional, and global computing environments.

6.2.4 Review annually the Service/Agency five-year IT investment strategies for their programs for alignment of priorities and synchronization of programs prior to the POM submission.

6.2.5 Provide for the elimination of duplicate personal, local, regional, and global computing centers within the Military Department or Defense Agency.

6.2.6 Establish certification authorities for personal and local computing architecture compliance.

6.2.7 Ensure all acquisition agents that develop or acquire applications or data of a regional or global nature use designated regional and global computing centers or obtain a waiver.

6.2.8 Review all acquisitions of Enterprise Computing environments to ensure compliance with the approved IT investment strategy.

6.2.9 Implement consistent roles and responsibilities for personal and local computing service providers including specific performance measurements.

6.2.10 Establish a process for selecting, evaluating and accrediting personal and local computing service providers.

6.2.11 Arbitrate issues regarding non-performance of SLAs for their Enterprise Computing service providers.

6.2.12 Create and maintain automated inventories of their current and planned personal, local, regional, and global computing capabilities and applications.

6.2.13 Report annually the status of the Enterprise Computing environment to the DoD CIO.

6.3 DoD and Service/Agency Enterprise Computing Acquisition Agents

6.3.1 Gather and aggregate requirements for Enterprise Computing environments to support applications and user access.

6.3.2 Select the appropriate standard configurations for Enterprise Computing environments based on BCAs.

6.3.3 Obtain certification of Enterprise Computing architecture compliance from the designated certification authority.

6.3.4 Plan and resource the acquisition and implementation of required personal, local, regional, and global computing capabilities and capacities.

6.3.5 Oversee the acquisition of Enterprise Computing capabilities or the selection of the computing service providers.

6.3.6 Establish SLAs between the computing service providers and users.

6.3.7 Ensure configuration management of Enterprise Computing environments is established and maintained.

6.3.8 Evaluate the performance of all Enterprise Computing environments for their user base.

6.3.9 Ensure all software is appropriately licensed.

6.3.10 Evaluate performance of computing providers and oversee contracts including the providers' SLAs.

6.3.11 Take appropriate action with providers for not meeting the performance requirements of the SLA.

6.4 Joint and Service/Agency Application Acquisition Agents will

6.4.1 Gather functional and operational requirements for Enterprise Computing for their applications.

6.4.2 Select the appropriate standard application program interfaces with their associated standard computing configurations for each application based on BCAs.

6.4.3 Obtain certification of Enterprise Computing architecture compliance from the designated certification authority.

6.4.4 Ensure all software is appropriately licensed.

6.4.5 Plan and resource any additional personal, local, regional, and global computing capabilities or capacities needed to support their applications. The Enterprise Computing acquisition agent(s) and application acquisition agents must coordinate the provision of the additional capabilities or capacities, as needed.

6.5 Enterprise Computing Service Providers will:

6.5.1 Obtain accreditation from the appropriate CIO.

6.5.2 Deliver specified services in accordance with the SLA.

6.5.3 Report performance measures as specified.

6.5.4 Provide visibility of the Enterprise Computing operational status to the appropriate GIG operators and users.

6.5.5 Ensure that appropriate backup and recovery capabilities are in place to assure continuity of operations.

6.5.6 Maintain secure Enterprise Computing environments.

6.5.7 Ensure all software is appropriately licensed.

6.5.8 Maintain configuration management of all their Enterprise Computing environments and an inventory of all related assets.

7 EFFECTIVE DATE: This directive is effective immediately upon issuance and until superseded.

Enclosure (1) - Computing and Communications Architecture Framework Sub-View

The Computing and Communications Architectural Framework (CCAFS), shown in Figure A-1 below, was used in formulating the directives contained in this Policy and Guidance Memorandum. The CCAFS is used to identify and describe the various components that comprise an enterprise-wide information technology infrastructure to address the functional requirements of Joint and Service/Agency applications across all operational environments. This information technology infrastructure supports the capture, processing, transmission, storage, and retrieval of enterprise information in all forms and provides secure, interoperable, and manageable IT capabilities for the Global Information Grid (GIG).

The CCAFS exists as a Sub-view within the Systems View of the proposed Enterprise Architecture Framework (EAF). The EAF is positioned as an extension to the C4ISR Architecture Framework Version 2. The EAF and the CCAFS will require formal review and adoption by the Architecture Coordination Council (ACC). The CCAFS is presented here to provide a common conceptual representation and definitions of the components of the GIG Computing and Communications Capability for DoD for use in describing related policies.

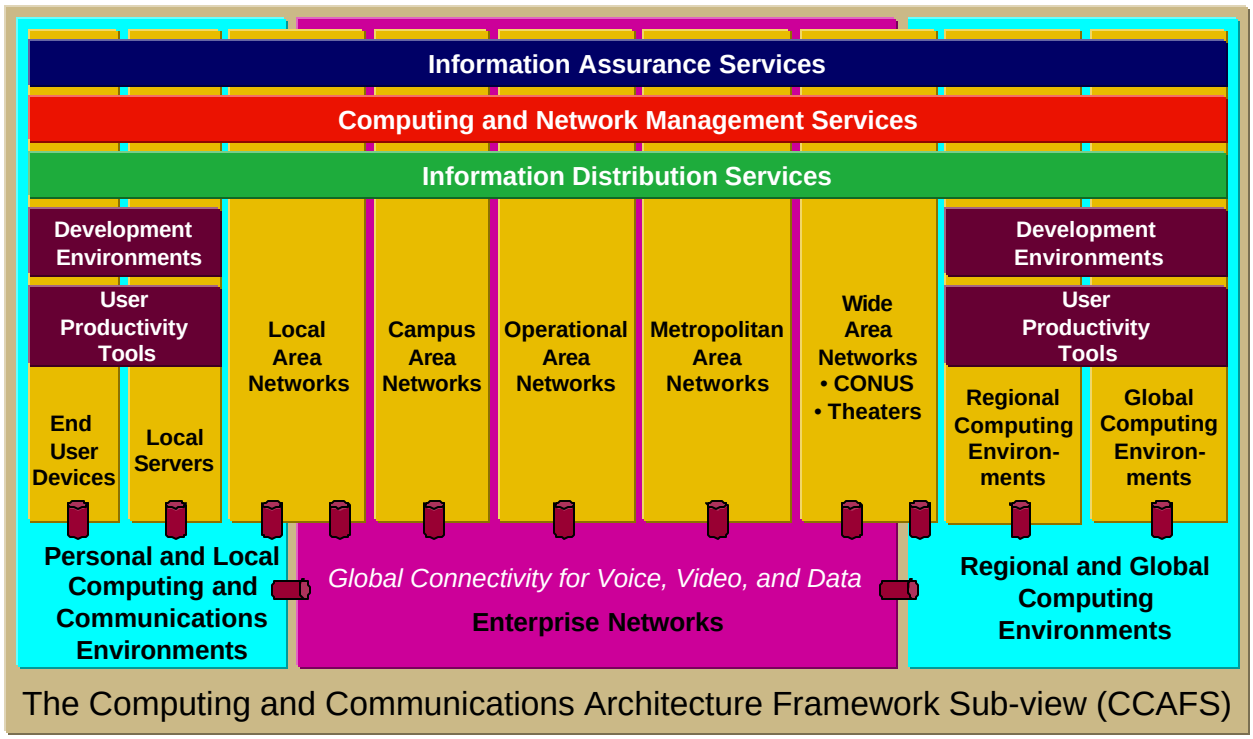

Figure A-1: The Computing and Communications Architecture Framework Sub-view

The Computing and Communications Architecture Framework Sub-view contains the architecture elements needed to identify required IT infrastructure capabilities and to develop architectural solutions to deliver those capabilities. It is organized around both a technological and topological orientation. The three bands across the top of the CCAFS are of particular

importance since they represent the necessary end-to-end capabilities for inter-operability of information assurance, management, and information distribution services.

Personal and Local Computing and Communications Environments contains those elements that provide localized capabilities to users of the infrastructure. It includes all types of end-user devices for access and retrieval of information and services provided by the GIG. It also includes local servers and the associated Local Area Networks to interconnect all local devices. It is used to develop standard solutions for local computing capabilities across various types of DoD facilities, operational platforms (ships, planes, tanks, etc.), and mobile user communities (expeditionary and deployed forces). It includes the user productivity tools required to support the inter-working of remotely located personnel connected to the appropriate Enterprise Network. Local Servers and Local Area Networks (LANs) are included in the Local Computing Architecture as they are typically designed and managed in conjunction with end-user devices and local operational requirements.

Personal and Local Computing and Communications Environments are connected to Enterprise Networks through appropriate communications adapters or gateways depending on their locations. Deployed platforms and units use Operational Area Networks (OANs) based on wireless technologies to support localized communication and provide access to Theater-based Wide Area Networks using satellite communications. Fixed facilities link through Campus Area Networks (CANs) when they are part of a base, camp, post, garrison, or other type of military installation. Campuses and isolated facilities in areas of high concentration of military installations use Metropolitan Area Networks (MANs) to support intra-regional traffic and provide gateways to the enterprise Wide Area Networks (WANs). CONUS and Theater-based WANS combine to provide a global backbone connectivity capability.

Various types of Enterprise Networks are constructed from these five network components (LANs, OANs, CANs, MANs, and WANs). These Service Networks provide the necessary level of secure networking capability to support all types of information exchange and distribution between end user devices and with the application and information servers.

Regional and Global Computing Environments operate across the Enterprise Service Networks. Regional Computing Environments support applications where data is distributed on a regional basis and Global Computing Environments support applications where data is best centrally managed. Both types of Regional and Global Computing Environments offer a similar range of technical environments for application and information processing.

This Enterprise Computing Policy relates directly to the Personal and Local Computing and Communications Environments and the Regional and Global Computing Environments as represented in this CCAFS.

Enclosure (2): Definitions

Acquisition Agent is any program manager or DoD authorized purchaser that buys GIG products and services and also manages these resources over their life cycle.

Business Case Analysis is the evaluation of alternative solutions that includes the ability to meet the defined requirements (e.g., technical, functional, training, implementation, operational, and scheduling), total cost of delivery and sustainment, operational performance considerations, and associated risks.

Computing and Communications Capability comprises local computing environments, enterprise networks, and regional and global computing environments and related information assurance management, infrastructure management, and information distribution services.

Computing and Network Management Services include performance management, configuration management, change management, operating systems management, help desk tools and services, service scheduling, backup and recovery management, and usage and cost accounting.

Development Environment includes compilers, interpreters, CASE tools, debuggers, web publishing tools, and modeling, simulation and analysis tools.

End User Devices are personal computers including desktop and laptops, thin clients, high-end workstations, personal digital assistants, telephones, and pagers.

Enterprise includes the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities.

Enterprise Computing comprises personal, local, regional and global computing environments.

Enterprise Computing Coordinator is the single point of contact on a military or civilian installation or facility that is responsible for the connectivity of the end user devices, local servers and local networks.

Enterprise Networks are comprised of all Service and Transport networks and telecommunications services as designated by the DoD CIO Executive Board.

Global Computing Center is an operations facility (e.g., Defense Megacenter) supporting global computing environments of all required types of platforms providing centralized computing services for the enterprise.

Global Computing Environment is a computing capability that supports centralized application or data processing for the enterprise.

Global Information Grid (GIG) The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary

to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

Information Assurance Services include encryption, access control, user identification and authentication, malicious content detection and virus protection, audit, physical and environment controls, computer assisted downgrading, Public Key Infrastructure, and certificate management.

Information Distribution Services include directory services, electronic mail transport, network news transport, web transport, file transfer services, voice and video conferencing, broadcasting services, network time services, domain name services, and remote procedure calls.

Information Technology means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Joint Applications are functional systems that are used by multiple Services and/or Agencies.

Legacy Environments include non-standard, non-compliant technologies and obsolete applications and Computing and network.

Local Computing Environment is a combination of local servers, shared peripherals, local networks, user productivity tools and associated software available at a given work site, which may be fixed, mobile, or deployable.

National Security Systems means any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions.

Personal Computing Environment is a combination of end user devices, peripherals, user productivity tools and associated software available at a personal work location, which may be fixed, mobile, or deployable.

Regional Application is a functional system or component where the data is accumulated for a regional operating area and the users are largely based within that region.

Regional Computing Center is an operations facility supporting regional computing environments of all required types of platforms providing computing services to a regional operating area.

Regional Computing Environment is a computing capability that supports application processing for information that is applicable to a specific geographic region and includes the following types of servers: application, web, database, document, video, mail, and print.

Regional and Global Computing Environment is a combination of computing platforms,

peripherals, user productivity tools and associated software that are accessed via enterprise networks

Service/Agency Applications are functional systems that are used by individual Services or Agencies.

Service Level Agreement is any type of management vehicle between a service provider and a customer that specifies performance requirements, measures, reporting, cost, and recourse.

Service Provider is any type of organization internal or external to DoD who has designated responsibility for the operation of one or more components of the Global Computing and Networking Capability.

Standard Configuration is a template providing a common, reusable design of technology components within the overall GIG Computing and Communications Capability. These design templates include all required elements of hardware and software excluding applications systems. They are defined for different types of local computing environments, enterprise networks, and regional and global computing environments.

User Productivity Tools include document processing, spreadsheet, presentation graphics and personal database, email, world wide web browser, collaborative computing, calendar management and scheduling, application clients, digital telephony, video and audio conferencing and voice mail.

September 30, 1999

GNIE Enterprise Computing Team

Lt Col Ron Holloway, OSD(C3I), Co-Chair
Dale Christensen, Navy/Office of DON CIO, Co-Chair
Patty Bodenstein, Army/Office of Army CIO
CMSgt Ray Kennedy, Air Force/AFCIC
Jerry Lelansky, DLA
Mary Lynn West, DFAS
Alfred Rivera, DISA
Jeanette Carter, DISA
Art Caston, A.T. Caston Consulting
Emil DeRenzo, MITRE (DIA/IC representative)
Jeff Rogers, MITRE
John Machado, Machado Associates